



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/028,573	12/19/2001	Eric Klingler	CING-0619/769.US	3290
54499 7590 01/08/2008 WOODCOCK WASHBURN LLP CIRA CENTRE 12th Floor 2929 ARCH STREET PHILADELPHIA, PA 19104-2891			EXAMINER PYZOCHA, MICHAEL J	
			ART UNIT 2137	PAPER NUMBER
			MAIL DATE 01/08/2008	DELIVERY MODE PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No. 10/028,573	Applicant(s) KLINGLER ET AL.	
	Examiner Michael Pyzocha	Art Unit 2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 30 October 2007.
- 2a) ☐ This action is FINAL. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-5, 18-28 and 30 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-5, 18-28 and 30 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

Art Unit: 2137

DETAILED ACTION

1. Claims 1-5, 18-28, and 30 are pending.
2. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 10/30/2007 has been entered.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claim 1 is rejected under 35 U.S.C. 103(a) as being unpatentable over Albert et al. (US 5991410) in view of Eftimakis et al (US 5889781) in view of Ayanoglu (US 5717689) and further in view of Dupuy et al. (US 5613203).

Art Unit: 2137

As per claim 1, Albert et al. discloses processing a message for transmission, wherein the message includes control data and payload data, and wherein the control data is not encrypted and contains a particular control message wherein the control data is used to provide at least one other function related to the wireless communication (see column 16 lines 39-67 column 17 lines 12-23); detecting the particular control message (see column 16 lines 55-59); initializing the cryptosystem, using the cryptosystem to encrypt the message for transmission (see column 16 lines 55-67); receiving a message, including unencrypted control data and encrypted payload data, parsing the message for transmission to separate the unencrypted control data from the payload data; determining whether the control data contains the particular control message (see column 17 lines 17-20); if the unencrypted control data contains the particular unencrypted control message initializing the cryptosystem using the key and decrypting the payload data (see column 17 lines 17-23).

Albert et al. fails to disclose the counter, the use of an encrypted airlink packet for transmission over an airlink and the control message indicates that a process of establishing a wireless communication connection is being completed.

Art Unit: 2137

However, Eftimakis et al. teaches a counter (see column 7 lines 3-18), Ayanoglu teaches the use of an airlink packet (see column 22 lines 43-49), and Dupuy et al. teaches including a message (a SABM message) indicating the process of establishing a wireless communication connection is being completed (see column 1 lines 42-53).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use the counter of Eftimakis et al, the SABM message of Dupuy et al. and the airlink packet of Ayanoglu in the Albert et al. system.

Motivation to do so would have been to locate the synchronization information (see Eftimakis et al column 7 lines 3-18) to provide built in CRC for error detection (see column 22 lines 43-49) and to show acknowledgment of the connection (see Dupuy et al. column 1 lines 42-53).

Eftimakis et al teaches the counter starting at zero and ending at 49, however one of ordinary skill in the art would know a counter can be decremented to obtain the same results.

5. Claim 2 is rejected under 35 U.S.C. 103(a) as being unpatentable over the modified Albert et al., Eftimakis et al and Ayanoglu system as applied to claim 1 above, and further in view of Bender (US 6366779).

Art Unit: 2137

As per claim 2, the modified Albert et al., Eftimakis et al, Ayanoglu and Dupuy et al. system fails to disclose the control message is a link control channel message.

However, Bender teaches such a message (see column 14 lines 38-62).

At the time of the invention it would have been obvious to a person of ordinary skill in the art for the modified Albert et al., Eftimakis et al, Ayanoglu and Dupuy et al. system's control message to be a link control channel message.

Motivation to do so would have been to allow the base station to initiate a call (see column 14 lines 38-62).

6. Claims 3 and 5 are rejected under 35 U.S.C. 103(a) as being unpatentable over the modified Albert et al., Eftimakis et al, Ayanoglu and Dupuy et al. system as applied to claims above, and further in view of Schneier (Applied Cryptography).

As per claim 3, the modified Albert et al., Eftimakis et al, Ayanoglu and Dupuy et al. system fails to disclose the use of a state box.

However, Schneier teaches such a state box (see pages 397-398).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use Schneier's state

Art Unit: 2137

box as the cryptosystem of the modified Albert et al., Eftimakis et al, Ayanoglu and Dupuy et al. system.

Motivation to do so would have been the simplicity of the algorithm (see page 398).

As per claim 5, the modified Albert et al., Eftimakis et al, Ayanoglu, Dupuy et al. and Schneier system discloses a RC4 state box and key (see Schneier pages 397-398).

7. Claim 4 is rejected under 35 U.S.C. 103(a) as being unpatentable over the modified Albert et al., Eftimakis et al, Ayanoglu, Dupuy et al. and Schneier system as applied to claim 3 above, and further in view of Lynn (US 5345508).

As per claim 4, the modified Albert et al., Eftimakis et al, Ayanoglu, Dupuy et al. and Schneier system operating on a state box using the altered key, wherein the state box is an array of data (see Schneier pages 397-398) but fails to disclose discloses performing a mathematical operation on the key to alter the key for security, wherein the key is an array of data.

However, Lynn teaches performing a mathematical operation on the key (see Lynn column 2 lines 54-64).

At the time of the invention would have been obvious a person of ordinary skill the art use Lynn's method for initiating an encryption/decryption process in the modified

Art Unit: 2137

Albert et al., Eftimakis et al, Ayanoglu, Dupuy et al. and Schneier system.

Motivation to do so would have been to provide self-synchronization (see Lynn column 2 lines 47-51).

8. Claims 18-23 are rejected under 35 U.S.C. 103(a) as being unpatentable over the modified Albert et al., Eftimakis et al, Ayanoglu, Dupuy et al. and Schneier system as applied above, and further in view of Dent (US 5060266).

As per claims 18-19, the limitations are substantially the same as claim 1 with the addition of a state box, and are therefore taught as in claim 3, but fail to disclose the use of the ACC level.

However, Dent teaches the use of such level (see column 6 lines 43-60 and column 7 lines 12-31).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to perform the processing of the modified Albert et al., Eftimakis et al, Ayanoglu, Dupuy et al. and Schneier system at the ACC level.

Motivation to do so would have been to provide a "blank and burst" mode of operation (see column 7 lines 12-31).

As per claim 20, the modified Albert et al., Eftimakis et al, Ayanoglu, Dupuy et al., Schneier and Dent system discloses sending an encryption key (see Lynn column 2 lines 54-64).

Art Unit: 2137

As per claim 21, the modified Albert et al., Eftimakis et al, Ayanoglu, Dupuy et al., Schneier and Dent system discloses changing the encryption key according to a predetermined algorithm (see Lynn column 2 lines 54-64).

As per claim 23, the modified Albert et al., Eftimakis et al, Ayanoglu, Dupuy et al., Schneier and Dent system discloses the method being performed each time the base station participates (see Albert et al. column 16 lines 36-67).

As per claim 22, the modified Albert et al., Eftimakis et al, Ayanoglu, Dupuy et al., Schneier and Dent system discloses the method being performed at the associated control channel level (see Dent column 6 lines 43-60 and column 7 lines 12-31).

9. Claim 24 is rejected under 35 U.S.C. 103(a) as being unpatentable over the modified Albert et al., Eftimakis et al, Ayanoglu, Dupuy et al. Schneier and Dent system as applied to claim 18 above, and further in view of Bender.

As per claim 24, the modified Albert et al., Eftimakis et al, Ayanoglu, Dupuy et al. Schneier and Dent system discloses the use of a SABM message, but fails to disclose the particular control message is a link control channel ("LCC") message.

However, Bender teaches the LCC message (see column 14 lines 38-62).

Art Unit: 2137

At the time of the invention it would have been obvious to a person of ordinary skill in the art for the messages of the modified Albert et al., Eftimakis et al, Ayanoglu, Dupuy et al., Schneier and Dent system to be those of Bender.

Motivation to do so would have been to allow the base station to initiate a call (see Bender column 14 lines 38-62).

10. Claims 25 and 30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Albert et al. in view of Malek et al. (US 5243653) in view of Dent and further in view of Dupuy et al.

As per claim 25, Albert et al. discloses at least one digital signal processing means; at least one central processing means; and encryption synchronization means configured to detect a particular control message in a data transmission wherein the control data is used to provide at least one other function related to the setup of a wireless communication (see column 16 lines 39-67), wherein the particular control message is used according to a wireless communication protocol to provide at least one other control function under the wireless communication protocol and, in response, wherein the particular control message occurs just before the transmission of data (see columns 16 and 17 as applied above).

Albert et al. fails to disclose the method being performed at the associated control channel level for telephony data and

Art Unit: 2137

the control message indicates that a process of establishing a wireless communication connection is being completed.

However, Dent teaches the use of such level (see column 6 lines 43-60 and column 7 lines 12-31) Malek et al. teaches telephony data (see column 4 lines 47-57) and Dupuy et al. teaches including a message (a SABM message) indicating the process of establishing a wireless communication connection is being completed (see column 1 lines 42-53).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to perform the processing of the Albert et al. system on telephony data at the ACC level.

Motivation to do so would have been to provide a "blank and burst" mode of operation (see Dent column 7 lines 12-31) to provide a system that does not degrade the voice quality (see Malek column 2 lines 6-15) and to show acknowledgment of the connection (see Dupuy et al. column 1 lines 42-53).

As per claim 30, the modified Albert et al., Dent, Malek and Dupuy et al. system discloses the initiation of the encryption/decryption process occurs each time a wireless connection is set up, comprising initial connection, connection hand off, and connection reestablishment after unexpected connection loss (see Malek column 4 lines 47-57).

Art Unit: 2137

11. Claims 26 and 27 are rejected under 35 U.S.C. 103(a) as being unpatentable over the modified Albert et al., Dent, Malek and Dupuy et al. system as applied to claim 25 above, and further in view of Lynn et al.

As per claim 26, the modified Albert et al., Dent, Malek and Dupuy et al. system fails to disclose the encryption synchronization means is further configured to provide a current encryption key to receiving devices and sending devices in the wireless communication network.

However, Lynn teaches such synchronization (see column 2 lines 47-51 and column 5 line 40 through column 6 line 23).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to perform the synchronization of Lynn in the modified Albert et al., Dent, Malek and Dupuy et al. system.

Motivation to do so would have been to not require additional recovery procedures (see Lynn column 2 lines 47-51).

As per claim 27, the modified Albert et al., Dent, Dupuy et al., Malek and Lynn system discloses the encryption synchronization means is further configured to count data blocks in a message being transmitted to determine when to begin encryption/decryption (see Lynn column 5 line 40 through column 6 line 23).

12. Claim 28 is rejected under 35 U.S.C. 103(a) as being unpatentable over the modified Albert et al., Dent, Malek, Dupuy et al. and Lynn system as applied to claim 26 above, and further in view of Schneier (Applied Cryptography).

As per claim 28, the modified Albert et al., Dent, Malek, Dupuy et al. and Lynn system fails to disclose the use of a state box.

However, Schneier teaches such a state box (see pages 397-398).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use Schneier's state box as the cryptosystem of the modified Malek, Lynn, and Dent system.

Motivation to do so would have been the simplicity of the algorithm (see page 398).

Response to Arguments

Applicant's arguments filed 10/30/2007 have been fully considered but they are not persuasive. Applicant argues the cited references fail to teach a control message indicating the process of establishing a wireless communication connection is being completed; and Albert fails to disclose initializing a

Art Unit: 2137

cryptosystem with a key when the control data contains a specific message.

Applicant's argument that the cited references fail to teach a control message indicating the process of establishing a wireless communication connection is being completed is moot in view of the new grounds of rejection.

With respect to Applicant's argument that Albert fails to disclose initializing a cryptosystem with a key when the control data contains a specific message, when the encryption flag is initially set the data is encrypted. In order for this encryption to take place the cryptosystem must be initialized with the key used for this encryption. Furthermore, the wireless adapter receives the frame with the encryption flag is must use the same algorithm (as described in column 17 lines 20-23) and the same key in order to obtain the plaintext of the encrypted text. Therefore, this cryptosystem must also be initialized with the key.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael Pyzocha whose telephone number is (571) 272-3875. The examiner

Art Unit: 2137

can normally be reached on 7:00am - 4:30pm first Fridays of the bi-week off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

MJP


EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER